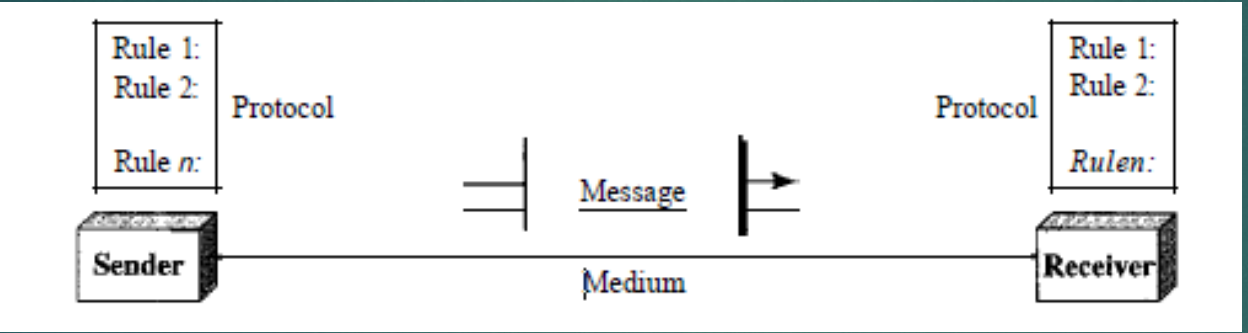
Unit-1
Introduction to Communication

PREPARED BY: SUSHANT BHATTARAI

Components

- A data communications system has five components:



- Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- Sender: The sender is the device that sends the data message. It can be a computer , workstation, telephone handset, video camera, and so on.

Components

- Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation

- Information today comes in different forms such as text, numbers, images, audio, and video.
- Text
  - In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.
- Numbers
  - Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Data Representation

- Images
  - Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.
- Audio
  - It refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.
- Video
  - Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow or Modes of Communication

- Simplex
- Half-duplex
- Duplex(Full duplex)

Simplex

- The transmission is possible in only one direction
- Can either send or receive data
- Example: Television, Radio, etc.

Half-Duplex

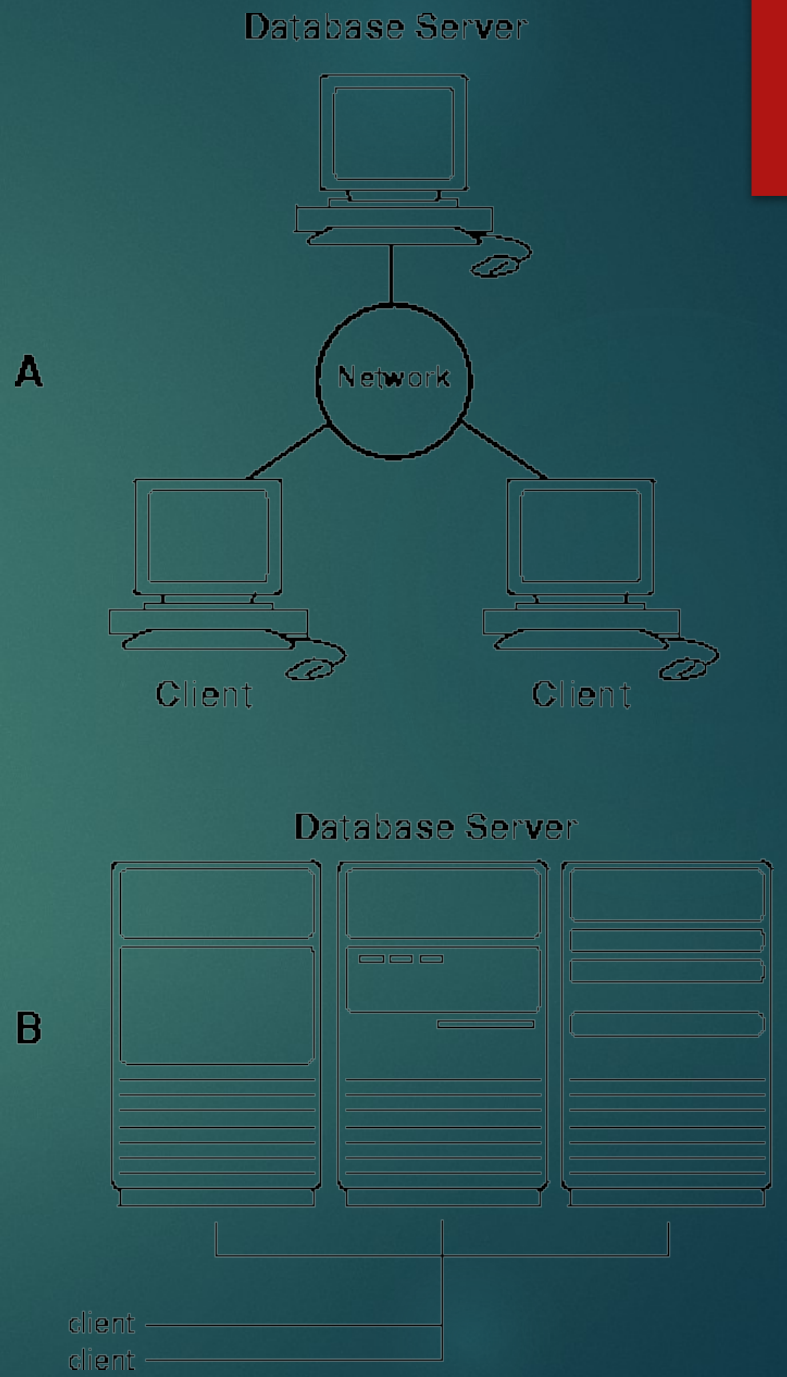
- Communication is possible in both direction but not simultaneously.
- Only one device can send a data at a time.
- Example: Walkie-talkie, ATC and pilot,etc.

Full-duplex(Duplex)

- Communication is possible in both direction and simultaneously.
- Both device can send a data at a time.
- Example: Telephone , etc.

Distributed Processing

- Most networks use distributed processing, in which a task is divided among multiple computers.
- Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.



Network Criteria

- A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.
- Performance
  - Performance can be measured in many ways, including transit time and response time. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics: throughput and delay

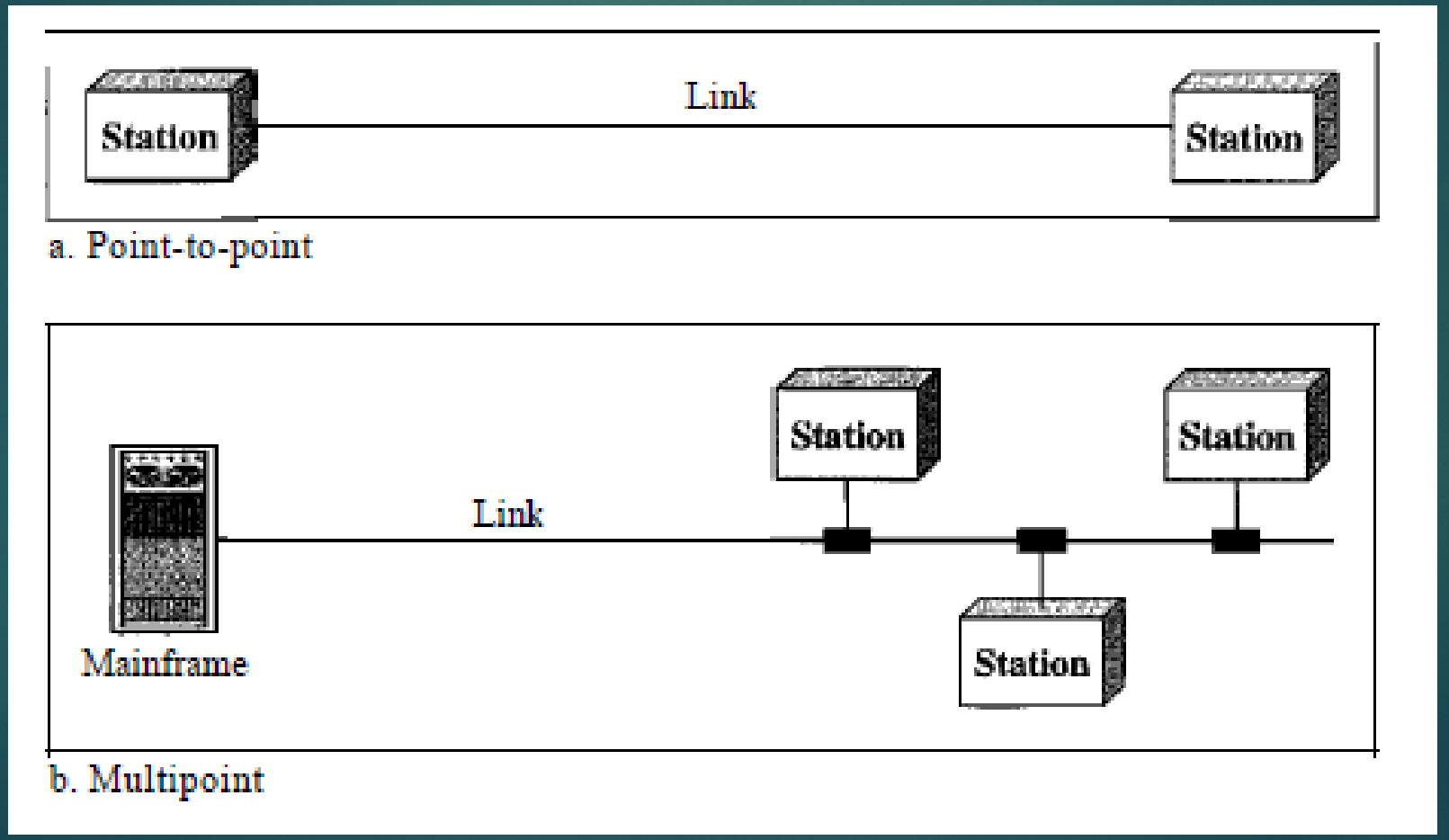
Network Criteria

- Reliability
  - In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.
- Security
  - Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Types of Connection

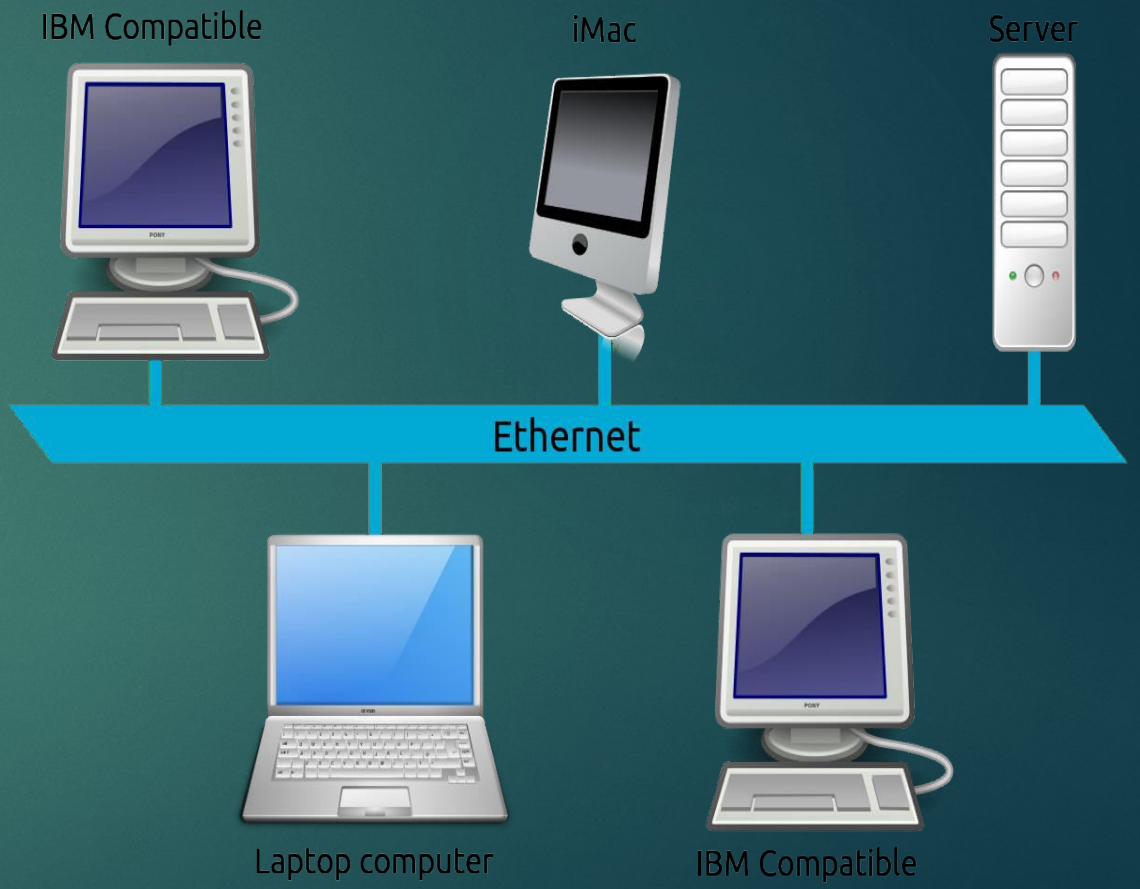
- Point-to-point:
  - A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.
- Multipoint:
  - A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link .In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

Types of Connection



LAN(Local Area Network)

- Contains printers, servers and computers
- Systems are close to each other
- Contained in one office or building
- Organizations often have several LANS



Advantages of LAN

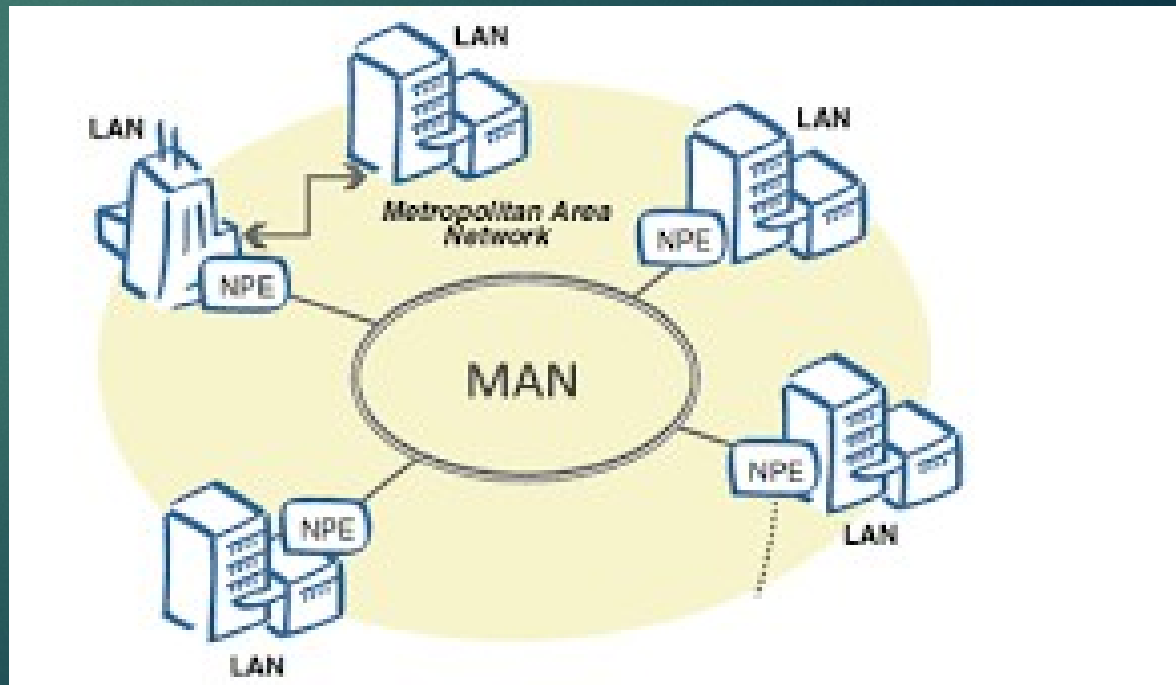
- Data transmission faster than MAN and WAN
- Higher security to resources
- Cheaper to establish
- Easier to establish , manage and operate

Disadvantages of LAN

- Limited to small area
- Connects comparatively less number of computers.
- Lack of Backup

MAN(Metropolitan Area Network)

- Large network that connects different organizations
- Shares regional resources
- A network provider sells time



Advantages of MAN

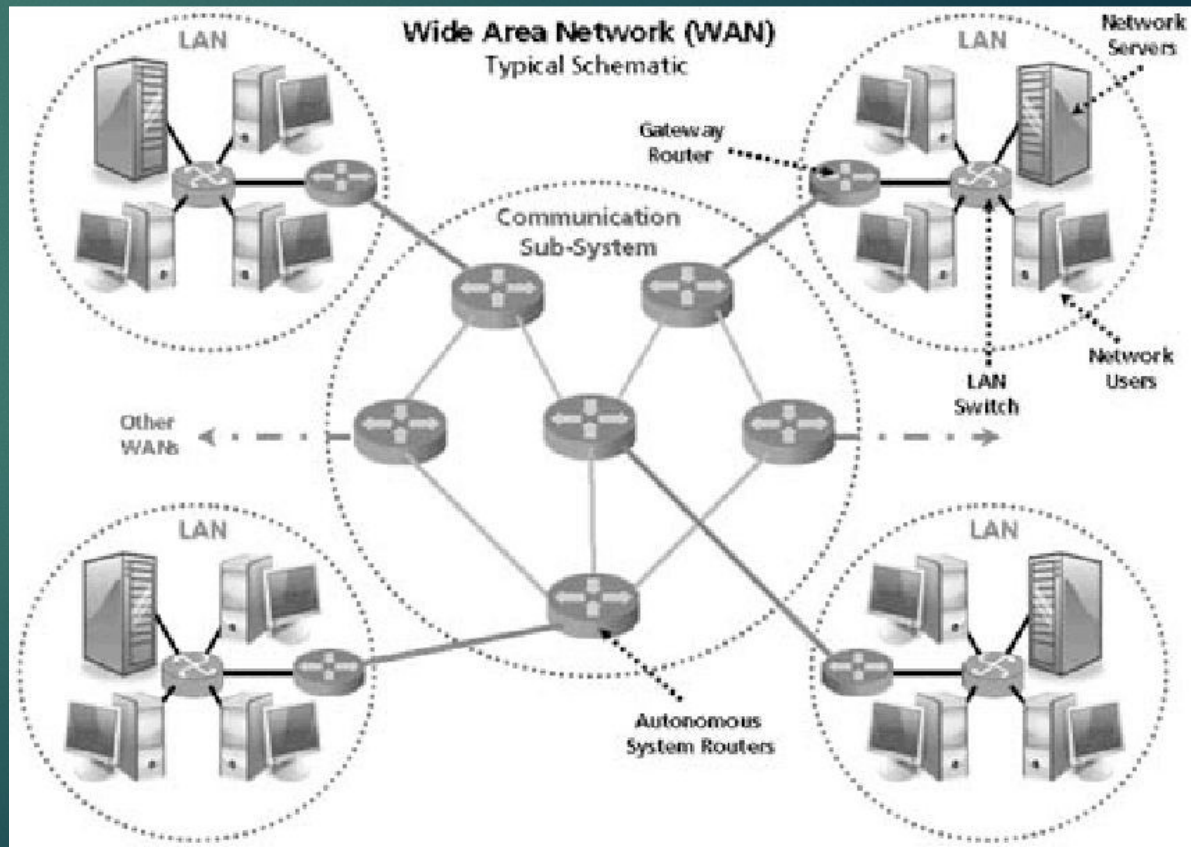
- Spread to a larger area than LAN
- Connects comparatively large number of computers than LAN
- Connects dissimilar networks

Disadvantages of MAN

- Uses comparatively expensive devices than used in LAN
- Low transmission speed
- Complex to establish
- Expensive to run

WAN(Wide Area Network)

- Two or more LANs connected
- Over a large geographic area
- Typically use public or leased lines
  - Phone lines
  - Satellite
- The Internet is a WAN



Advantage of WAN

- Spread large area than LAN and MAN
- Connects large number of computer
- Connects dissimilar network

Disadvantages of WAN

- Expensive
- Transmission speed low as compared to LAN
- Complex
- Highly qualified personnel required to manage , operate and establish

Network Topology

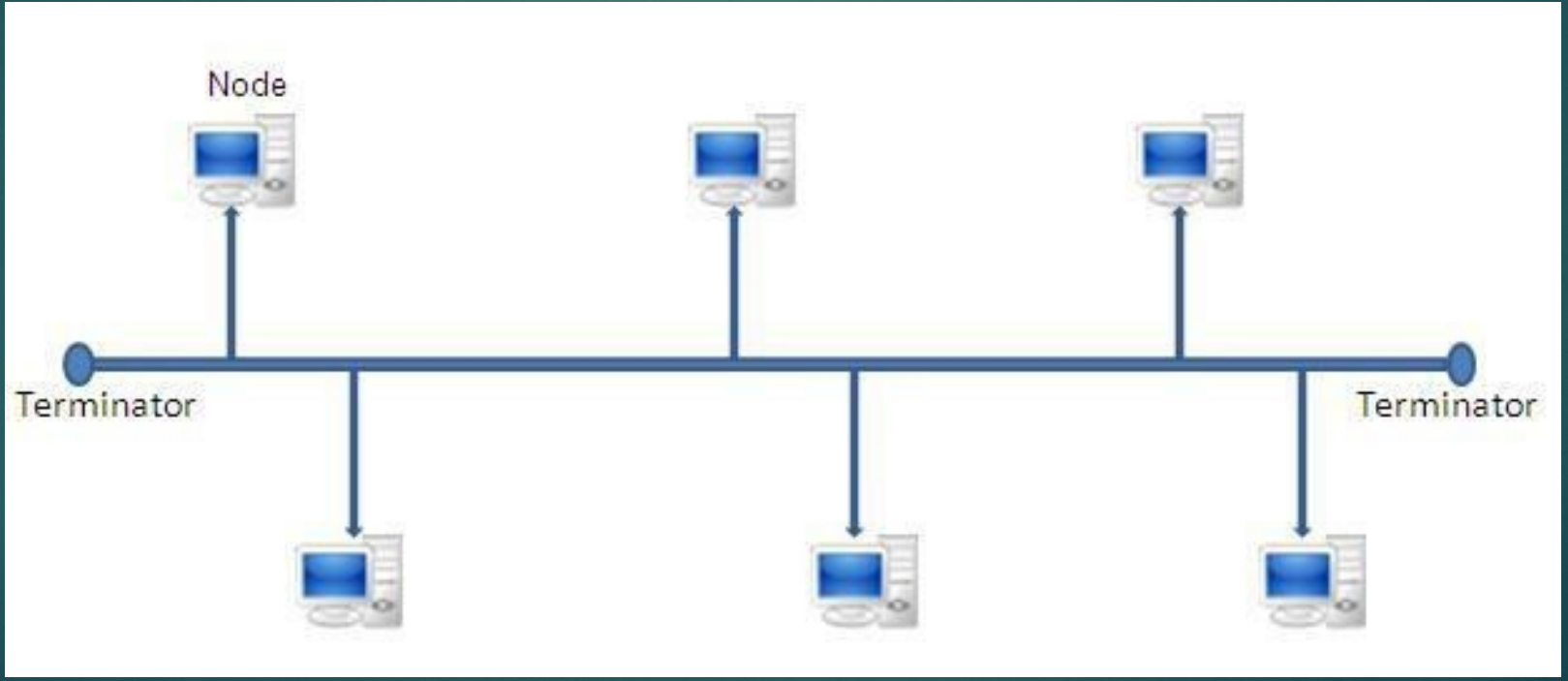
- The physical layout with geometrical arrangement of inter-connection of computer in a network is called network topology

Types of Network Topology

- Bus Topology
- Ring Topology
- Star Topology
- Tree Topology
- Mesh Topology
- Hybrid Topology

Bus Topology

- Bus topology connects each computer to a segment called trunk (bus).
- Coaxial cables are used.
- Consist of main cable with terminators at both ends.



Advantages of Bus Topology

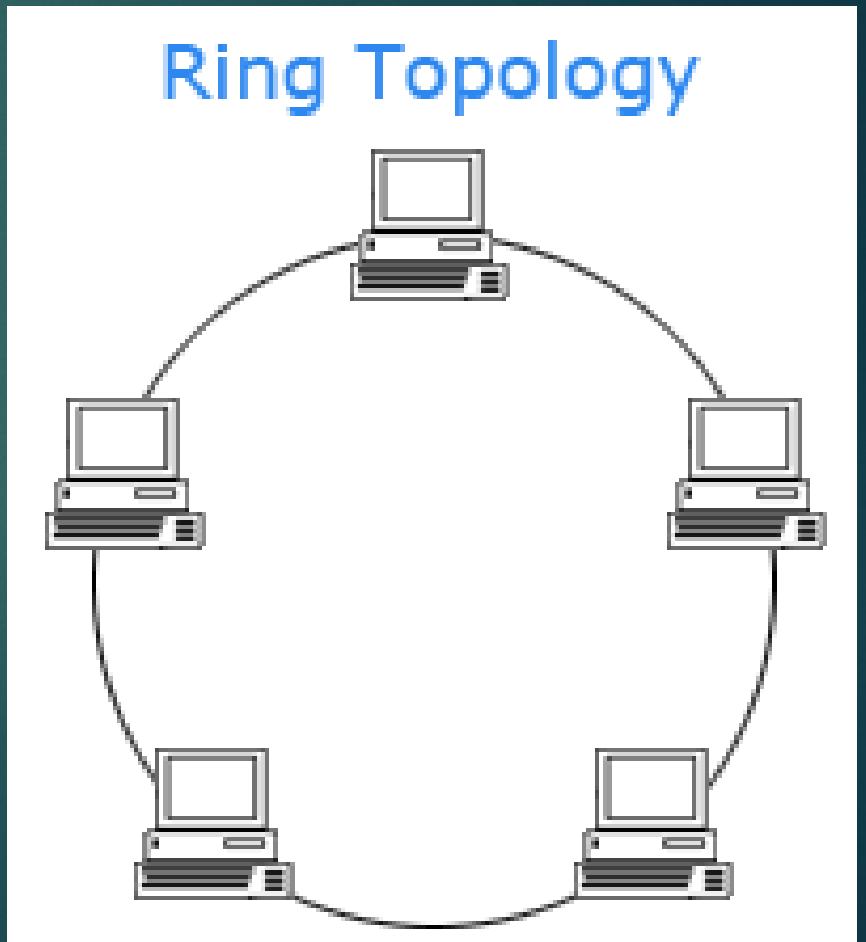
- Easy to setup
- Small amount of wire

Disadvantages of Bus Topology

- Slow
- Easy to crash
- Extension of PC will result in performance issue.

Ring Topology

- Nodes connected in a circle
- Tokens used to transmit data
- Nodes must wait for token to send
- Data transmission in high speed



Advantages of Ring Topology

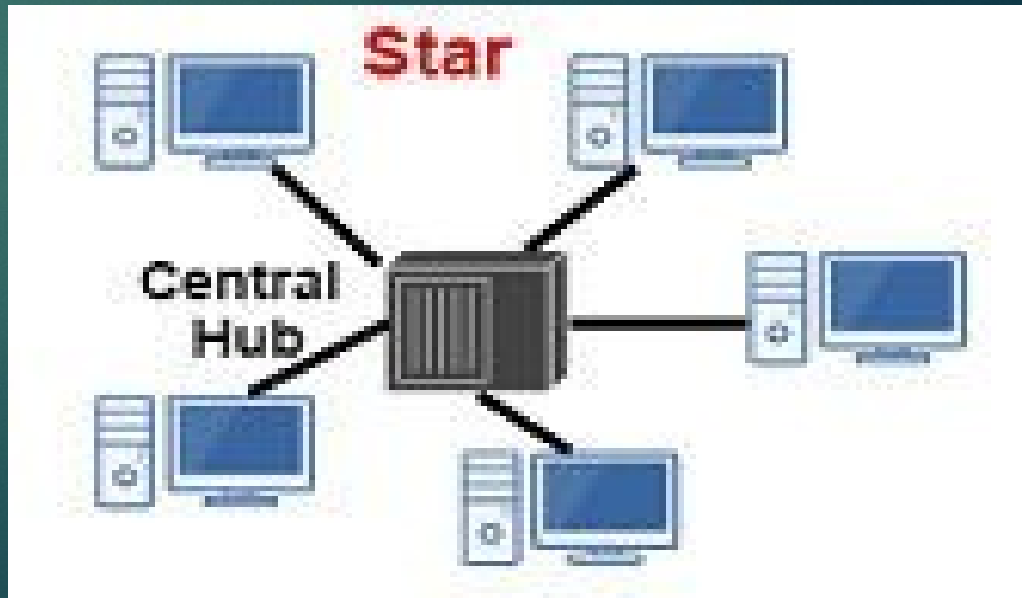
- Time to send data is known
- No data collisions
- High speed data transmission

Disadvantages of Ring topology

- Data can travel in only one direction
- Lots of cable
- Addition of computer is difficult
- If one computer is damaged, whole network fails to operate.

Star Topology

- Most common network topology found in most offices and home network.
- All nodes connect to a hub
  - Packets sent to hub
  - Hub sends packet to destination
- Hub amplifies the data signal & broadcasts it.
- High data traffic will be high which may increase data collision rate and data error rate.



Advantages of Star Topology

- Easy to setup
- One cable can not crash network
- Easier to add or remove computers.

Disadvantages of Star Topology

- One hub crashing downs entire network
- Uses lots of cable
- Most common topology

Networking Device

- Devices that are used to connect to are called network connecting devices
- Hub
- Switch
- Bridge
- Router
- Bridge

Hub

- Connectivity device with multiple ports.
- Used in star topology as a centrally connecting device.
- It accepts data from sender amplifies them and broadcasts.
- Cant impose the number of computer that can be connected.

Switch

- Considered to be an intelligent hub.
- Attempt to select the most direct path needed to send data packet to destination
- When data is received it creates a direct connection between sender and receiver and forwards the data packet to destination computer only.

Bridge

- A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.
- Bridge devices work at the data link layer of the Open System Interconnect (OSI) model
- Connecting two different networks together and providing communication between them.
- Bridges are similar to repeaters and hubs in that they broadcast data to every node.
- Bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.
- Bridges are also known as Layer 2 switches.

Router

- A router is a device like a switch the routes data packets based on their IP addresses.
- Router is mainly a Network Layer device.
- Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.
- Router divide broadcast domains of hosts connected through it.
- Operates in the network layer of OSI model.

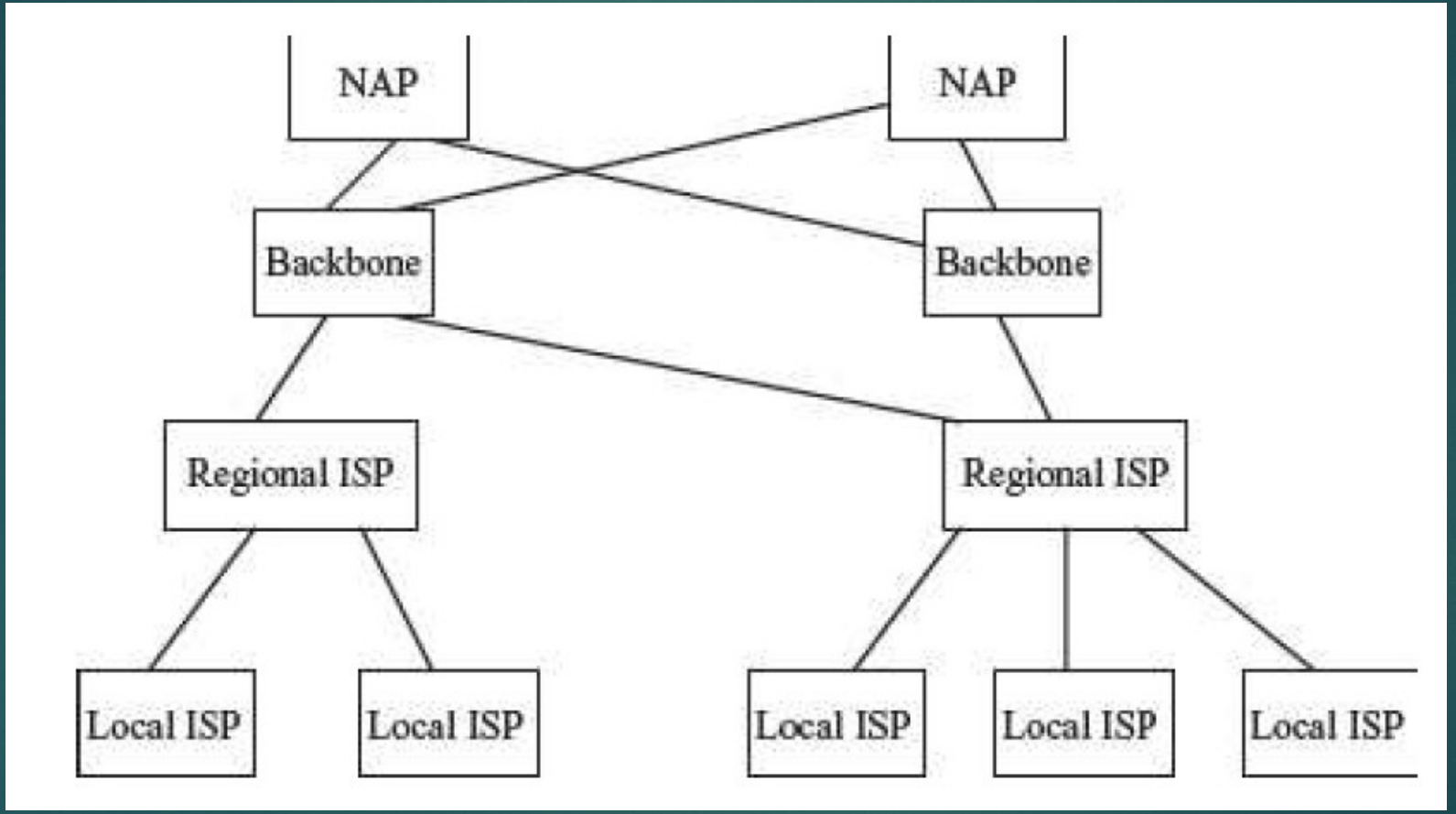
The internet architecture

- The architecture of Internet is hierarchical in nature.
- A brief description of the architecture of Internet is as follows:
- Client (user of computer) at home or in a LAN network is at the lowest level in hierarchy.
- Local Internet Service Provider (ISP) is at the next higher level.
  - An ISP is an organization that has its own computers connected to the Internet and provides facility to individual users to connect to Internet through their computers.
  - Local ISP is the local telephone company located in the telephone switching office, where the telephone of client terminates. Examples of local ISP in Nepal is Worldlink , Subisu , Classictech, CG Net,etc.
  - The client calls local ISP using a modem or Network Interface Card.

The internet architecture

- Regional ISP is next in the hierarchy. The local ISP is connected to regional ISP
  - A router is a special hardware system consisting of a processor, memory, and an I/O interface, used for the purpose of interconnecting networks. A router can interconnect networks having different technologies, different media, and physical addressing schemes or frame formats.
  - The regional ISP connects the local ISP's located in various cities via routers.
  - If the packet received by regional ISP is for a client connected to this regional ISP, then the packet is delivered; otherwise, packet is sent to the regional ISP's backbone.
- Backbone is at top of the hierarchy.
  - Backbone operators are large corporations like AT&T,UUNET,GTE Corp,etc. which have their own server farms connected to the backbone. There are many backbones existing in the world.
  - The backbone networks are connected to Regional ISP's with a large number of routers through high speed fiber-optics.
  - Network Access Point (NAP) connects different backbones, so that packets travel across different backbones.
  - If a packet at the backbone is for a regional ISP connected to this backbone, the packet is sent to the closest router to be routed to local ISP and then to its destination; otherwise, packet is sent to other backbone via NAP. The packet traverses different backbones until it reaches the backbone of regional ISP for which it is destined.

The internet architecture



The protocol

- It is the special set of rules that end points in a telecommunication connection use when they communicate.
- Protocols exist at several levels in a telecommunication connection.
- Example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level
- In Open Systems Interconnection (OSI), there are one or more protocols attach layer in the telecommunication exchange that both ends of the exchange must recognize and observe.
- Protocols are often described in an industry or international standard.

Syntax

- The term syntax refers to the structure or format of the data, meaning the order in which they are presented.
- example, some protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

- The word semantics refers to the meaning of each section of bits.
- How are a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- For example, does an address identify the route to be taken or the final destination of the message?

Timing

- The term timing refers to two characteristics: when data should be sent and how fast they can be sent.
- For Example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

- Standards are necessary in almost every business and public service entity
- The primary reason for standards is to ensure that hardware and software produced by different vendors can work together
- Without networking standards, it would be difficult if not impossible to develop networks that easily share information.
- Standards also mean that customers are not locked into one vendor.
- They can buy hardware and software from any vendor whose equipment meets the standard. In this way, standards help to promote more competition and hold down prices.

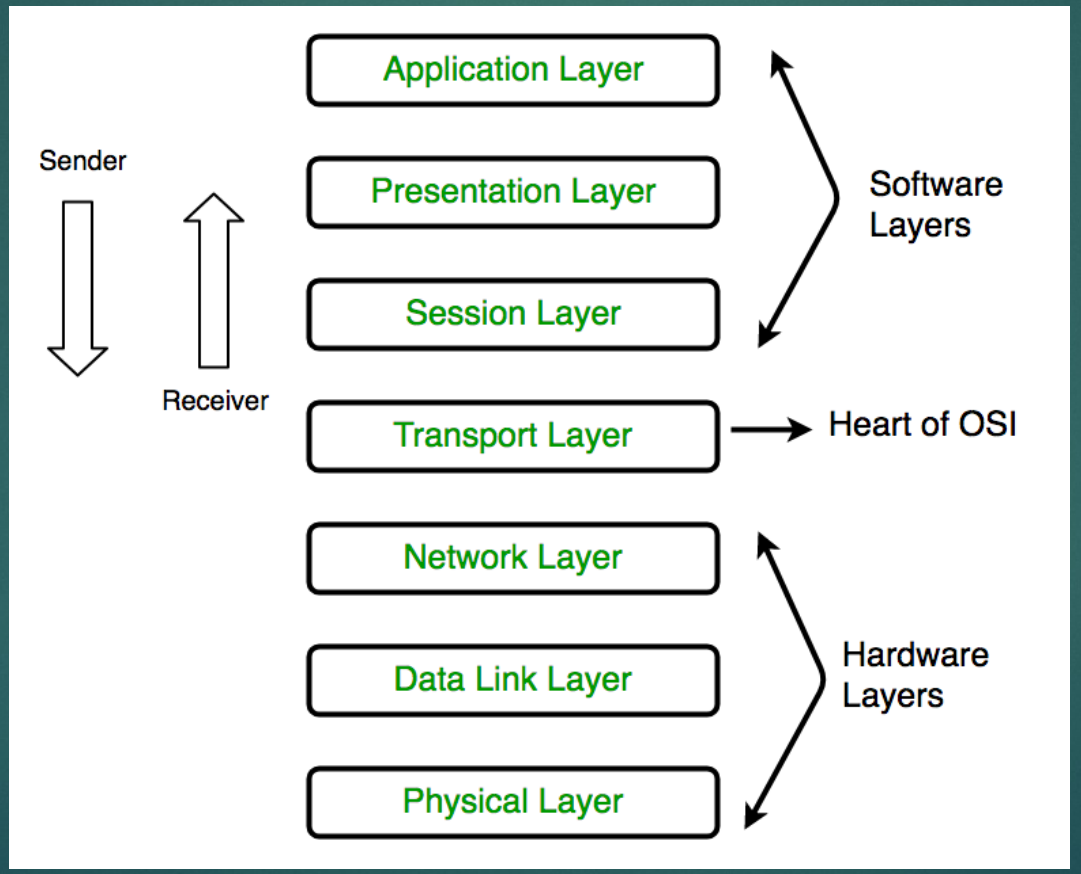
Standards

- There are two types of standards: de jure and de facto
- De jure standards, or standards according to law, are endorsed by a formal standards organization.
- The organization ratifies each standard through its official procedures and gives the standard its stamp of approval.
- De facto standards, or standards in actuality, are adopted widely by an industry and its customers.
- They are also known as market-driven standards. These standards arise when a critical mass simply likes them well enough to collectively use them.
- Market-driven standards can become de jure standards if they are approved through a formal standards organization.

OSI reference Model

- OSI stands for Open Systems Interconnection.
- It has been developed by ISO – 'International Organization of Standardization', in the year 1984.
- It is a 7 layer architecture with each layer having specific functionality to perform.
- All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

OSI reference Model



Physical Layer

- The lowest layer of the OSI reference model is the physical layer.
- It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of bits.
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer
- Data Link Layer will put the frame back together.

Data link Layer

- The data link layer is responsible for the node to node delivery of the message.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
- The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card).
- DLL also encapsulates Sender and Receiver's MAC address in the header.

Network Layer

- Network layer works for the transmission of data from one host to the other located in different networks.
- It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP address are placed in the header by the network layer.
- Functions:
  - **Routing:** The network layer protocols determine which route is suitable from source to destination.
  - **Logical Addressing:** The sender & receiver's IP address are placed in the header by network layer

Transport Layer

- Transport layer provides services to application layer and takes services from network layer.
- The data in the transport layer is referred to as Segments.
- It is responsible for the End to End Delivery of the complete message.
- Provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.
- At sender's side:
  - Transport layer receives the formatted data from the upper layers, performs Segmentation
  - Also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Transport layer

- At receiver's side:
- Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application.
- It also performs sequencing and reassembling of the segmented data.
- Functions :
- Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
- Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

Session Layer

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
- Functions:
- Session establishment, maintenance and termination
- Synchronization :
  - allows a process to add checkpoints which are considered as synchronization points into the data.
  - These synchronization point help to identify the error so that the data is resynchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
  - Dialog Controller : The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Presentation Layer

- Also called the Translation layer.
- The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
- functions of the presentation layer are :
  - Translation : For example, ASCII to EBCDIC.
  - Encryption/ Decryption : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
  - Compression: Reduces the number of bits that need to be transmitted on the network.

Application Layer

- At the very top of the OSI Model, we find Application layer which is implemented by the network applications.
- These applications produce the data, which has to be transferred over the network.
- This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
- Ex: Application – Browsers, Skype Messenger etc.

TCP/IP Model

- TCP/IP model, it was designed and developed by Department of
- Defense (DoD) in 1960s and is based on standard protocols.
- It stands for Transmission Control Protocol/Internet Protocol. The
- TCP/IP model is a concise version of the OSI model.
- It contains four layers, unlike seven layers in the OSI model.
- The layers are:
  - Process/Application Layer
  - Host-to-Host/Transport Layer
  - Internet Layer
  - Network Access/Link Layer

TCP/IP Model

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Network Access Layer

- This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model.
- It looks out for hardware addressing and the protocols present in thislayer allows for the physical transmission of data.

Internet Layer

- This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network.
- The main protocols residing at this layer are :
- IP – stands for Internet Protocol
- ICMP – stands for Internet Control Message Protocol.
- ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address.

Transport Layer

- This layer is analogous to the transport layer of the OSI model.
- It is responsible for end-to-end communication and error-free delivery of data.
- It shields the upper-layer applications from the complexities of data.
- ‘The two main protocols present in this layer are :
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)

Application Layer

- This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer.
- It is responsible for node-to-node communication and controls user interface specifications.
- Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP(Trivial FTP), Telnet, SSH(Secure Shell), SMTP, SNMP(Simple Network Management Protocol), NTP(Network Time Protocol), DNS

Addressing

- Four levels of addresses are used in an internet employing the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses